Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

Recommendation of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks	)))	EB Docket No. 06-119

COMMENTS OF AT&T INC.

CATHY CARPINO
GARY L. PHILLIPS
PAUL K. MANCINI

Attorneys For:
AT&T Inc.
1120 20th Street, NW
Suite 1000
Washington, D.C. 20036
(202) 457-3046 – phone
(202) 457-3073 – facsimile

August 07, 2006

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20054

Recommendation of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks	)))	EB Docket No. 06-119

COMMENTS OF AT&T INC.

AT&T Inc. ("AT&T"), on behalf of its telephone companies, hereby files these comments in response to the Notice of Proposed Rulemaking ("NPRM") in the foregoing docket.[1]

I. INTRODUCTION AND SUMMARY

AT&T commends the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks ("Panel") for both its comprehensive review of what happened to communications providers in the aftermath of Hurricane Katrina and its recommendations that, if implemented, will better prepare the communications industry and governmental entities for future disasters. AT&T also thanks the Commission for quickly responding to the needs of the industry in the days after Hurricane Katrina made landfall and for granting AT&T and others necessary prospective regulatory relief in the event of future disasters.[2] As recognized by both the Panel and the Commission, the stability of telecommunications infrastructure is essential to

---

[1] *Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, Notice of Proposed Rulemaking, EB Docket No. 06-119 (June 19, 2006).

[2] *See Petition of AT&T Inc. for Special Temporary Authority and Waiver to Support Disaster Planning and Response*, WC Docket No. 06-63, Order, DA 06-914 (rel. April 20, 2006) (granting AT&T limited Special Temporary Authority and waiver of the Commission's rules implementing section 272 to allow it to share network information, personnel, and facilities among its affiliates and across its region, and a waiver of the Commission's network disclosure rules); *see also Petition of BellSouth Corporation for Special Temporary Authority and Waiver to Support Disaster Planning and Response; Petition of Verizon for Special Temporary Authority and Waiver to Support Disaster Planning and Response; Petition of Qwest Communications International Inc. for Special Temporary Authority and Waiver to Support Disaster Planning and Response*, DA 06-1251, ¶ 2 (rel. June 9, 2006) (providing relief to Verizon, BellSouth, and Qwest and extending this additional relief to AT&T).

rescue efforts as well as to the protection and restoration of other critical infrastructures (*e.g.*, financial services). Indeed, as the Administration recently observed, the country relies on the communications industry, and other critical infrastructure industries, "to maintain [the nation's] defense, continuity of government, economic prosperity, and quality of life" and "their disruption [can] have a debilitating impact on national security, the economy, or public health and safety."[3]

Given its mandate, the Panel's recommendations were necessarily broad in scope. AT&T will focus its comments on recommendations affecting the telecommunications industry. For reasons provided below, AT&T supports the Panel's recommendation that industry consensus groups establish readiness checklists based on best practices and encourage their members to adopt them. AT&T also recommends that the Department of Homeland Security's National Coordinating Center for Telecommunications should continue to perform its role as the primary entity in the federal government for coordinating communications network recovery and information sharing among affected industry members. AT&T supports the Panel's recommendation that a nationally recognized credential be established and that employees and contractors of telecommunications infrastructure providers be designated as emergency responders. Finally, AT&T agrees with the importance of having diverse and redundant transport facilities, back-up power, and back-up Public Safety Answering Points to ensure the continued operation of the nation's 911 system during disasters. AT&T looks forward to working with the Commission to implement these recommendations.

[3] *Federal Response to Hurricane Katrina*, Lessons Learned, at 3, February 2006.

II. THE COMMISSION SHOULD DIRECT INDUSTRY CONSENSUS GROUPS TO ESTABLISH READINESS CHECKLISTS AND ENCOURAGE PROVIDERS TO ADOPT THEM.

About fifteen years ago, AT&T began its Network Disaster Recovery ("NDR") program because it too appreciated the importance of ensuring continuity of critical facilities – facilities relied on by government and key industries – in the event of a disaster.[4] Since that time, AT&T has invested more than $300 million in the program, which includes about 150 self-contained equipment-trailers and support vehicles for network element recovery and another 250 trailers that provide infrastructure back-up and logistical support (*e.g.*, power, air conditioning, first aid equipment, pumps, fuel, tools, and other infrastructure equipment). The NDR Operations team numbers around 60 employees who are specially trained restoration/recovery managers, engineers, and technicians located across the country. In addition to restoring its facilities, the NDR team has used its mobile satellite capabilities to provide communications support for humanitarian relief efforts and did so during the Hurricane Katrina disaster.

In the NPRM, the Commission seeks comment on the Panel's recommendation that the Commission work with and encourage each industry sector, through industry associations, to develop sector-specific readiness checklists to be followed in the event of a disaster.[5] AT&T supports this recommendation and suggests that the Commission require those communications entities that it regulates to develop and maintain a business continuity plan ("BCP") for significant service disruptions.[6] AT&T supports the Panel's recommendation that the Network

[4] *See* NPRM, Separate Statement of Deborah Taylor Tate (noting that AT&T and others have developed "extraordinary disaster recovery plans").
[5] NPRM ¶ 8 (citing Panel Report and Recommendations at 31).
[6] For example, the Pennsylvania Public Utility Commission requires carriers to submit a Public Utility Security Planning and Readiness Self Certification Form together with their annual financial or assessment report. As part of this filing, carriers do *not* provide a copy of their BCP or any other related plan. *See* http://www.puc.state.pa.us/general/onlineforms.aspx.

Reliability and Interoperability Council ("NRIC") develop a disaster readiness checklist for wireline carriers based on the industry's best practices, and AT&T agrees with the Panel on the checklist's contents.[7] AT&T looks forward to working with the next NRIC to develop this checklist, which should include such standard items as threat assessments and mitigation for various types of events (*e.g.*, earthquakes, flu pandemic), asset and service recovery prioritization, a command and control structure, coordination with key industry communications entities (*e.g.*, National Coordinating Center for Telecommunications or "NCC"), as well as a mechanism for testing and validating the efficacy of the program.

While AT&T agrees with the importance of a comprehensive readiness checklist, and AT&T's BCP includes the items detailed by the Panel in its recommendations, it is critical that companies continue to be afforded the discretion to determine what equipment must be kept in reserve (*i.e.*, what should be included in the cache of essential replacement equipment) and where and how to pre-position these assets. As mentioned above, AT&T has significant experience in this regard through its NDR program. AT&T maintains its NDR equipment at four undisclosed, geographically dispersed locations around the country. When appropriate, the company pre-positions these recovery assets to respond to disasters. For security reasons, the number of people within AT&T who are knowledgeable about the locations of these assets is purposefully kept to a minimum. And while AT&T will continue to have discussions with government officials about pre-positioning its NDR assets in advance of a pending disaster, AT&T would not support efforts to formalize these discussions by requiring AT&T to comply with staging requirements pursuant to published standards (*e.g.*, 50 miles from a particular location or expected event). Based on AT&T's experience, flexibility is key to a successful

[7] *See* Panel Report and Recommendations at 31. Similarly, NRIC should establish separate, best practices checklists for the wireless, cable, and satellite industries.

disaster recovery due to the variation in infrastructure assets being protected at different locations and the unique circumstances of different disaster scenarios. AT&T therefore recommends that the adoption of these best practices by carriers should be left to the carriers' discretion.

III. IMPORTANT COORDINATION WORK OF THE NCC MUST CONTINUE AND OUTAGE AND INFRASTRUCTURE REPORTING INFORMATION MUST BE KEPT CONFIDENTIAL.

In its report, the Panel explained that, under the National Response Plan, the lead federal agency for emergency support functions regarding communications is the National Communications System ("NCS"), which manages the NCC.[8] Established in 1984, the NCC is a joint industry-federal government partnership, which the Panel recognized "played an important and effective role [during Hurricane Katrina] in coordinating communications network recovery and allowing for information sharing among affected industry members."[9] The Panel noted that the NCC's current membership is limited and recommended that the Commission work with the NCS to broaden the NCC's composition to ensure adequate representation of all types of communications systems.[10] AT&T agrees with the Panel and supports broadening the NCC's membership to all interested communications providers.[11] The Panel also recommended that the Commission be the single point of collection for voluntarily provided outage and infrastructure information in the federal government during emergencies.[12] If this recommendation is implemented, AT&T asks that it be done in a manner that does not alter the NCC's role as the primary entity in the federal government for coordinating communications network recovery and information sharing among affected industry members.

---

[8] *Id.* at 19.
[9] *Id. See generally* http://www.ncs.gov/ncc/.
[10] Panel Report and Recommendations at 36.
[11] *Id.* at 19. We note that both Cox and Time Warner have membership requests pending with the NCS.
[12] *Id.* at 33-34.

AT&T strongly encourages the Commission and other federal agencies to work with the states and municipalities through their respective associations to educate state officials about their ability to obtain access to voluntarily provided outage and infrastructure data, in a manner that protects communications providers from public disclosure of sensitive information, so that companies do not have to duplicate their efforts in each state or, worse, comply with outage reporting obligations that vary by state or municipality. During a crisis, it is essential for communications providers to focus on restoration efforts and not have their resources diverted by having to respond to a multitude of state and local reporting requirements.[13] Moreover, permitting state and local government officials to contact just one place to obtain all of the outage and infrastructure information that they might need during a disaster frees up their scarce resources as well.

Disaster-Related Outage and Infrastructure Information. As suggested by the Panel, AT&T agrees that daily outage updates to the Commission are appropriate, unless, based on the exigencies of the situation, the Commission and providers find that more frequent updates would be useful. AT&T expects that the information it will voluntarily provide will be limited to the status of the service and infrastructure affected by the disaster (*i.e.*, it will not provide information about equipment in the disaster area that was unaffected or information about equipment outside of the disaster area).

AT&T also recommends that the Commission use its Network Outage Reporting System coupled with an Extensible Markup Language ("XML") application to facilitate data collection. Developing an XML application or a similar application will allow carriers to provide outage information on an automated basis (*i.e.*, upload outage information and update it automatically), which will dramatically shorten the amount of time required for data entry while allowing the

[13] *Id.* at 20.

Commission and other government agencies to receive this information sooner. To collect the additional data that may be voluntarily provided, AT&T strongly encourages the Commission to work with industry to develop the appropriate format and data fields. Ease of use is essential during a crisis, and the Commission should anticipate that, in some instances, this information may be provided to it over the telephone. Moreover, as noted by the Panel, it is important that the Commission not routinely alter the content, format, and frequency of these reports.[14] This is not a hypothetical concern. In the days following September 11, the recovery work being performed by AT&T's restoration personnel was frequently interrupted in order to respond to the changing reporting requirements of different levels of government.

Safeguards to Maintain the Confidentiality of Provider-Specific Data. The Panel recognizes the importance of protecting provider-specific data, even during an emergency.[15] Under Part 4 of the Commission's rules, communications providers in various industries (*e.g.*, cable, satellite, wireless, wireline) are required to report to the Commission information on certain outages.[16] Pursuant to Commission rules, this information is designated "not routinely available for public inspection"[17] and therefore "presumptively protected from public disclosure under the [Freedom of Information Act ("FOIA")]."[18] Thus, as a practical matter, under the Commission's rules, it is unlikely that state and local government officials would be able to gain access to the Commission's carrier-specific outage reports.[19]

---

[14] *See id.* at 34.
[15] *See id.*
[16] *See* 47 C.F.R. § 4.9.
[17] 47 C.F.R. §§ 4.2, 0.461.
[18] *See New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, ET Docket No. 04-35, Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 16830, 16853-55, ¶¶ 41-46 (2004).
[19] In its order expanding both the scope of its mandatory outage requirements and the classes of providers required to comply, the Commission emphasized how unlikely it would be for the Commission to grant a FOIA request seeking access to a carrier's outage report. *Id.*

Protected critical infrastructure information ("CII") that is voluntarily provided to the federal government, however, is expressly exempt from disclosure under FOIA.[20] In its interim rules implementing this statute, the DHS permits disclosure of protected CII to a state or local government entity only pursuant to the terms of its express written agreement with the DHS.[21] Absent appropriate confidentiality safeguards (*e.g.*, non-disclosure agreements), AT&T strongly agrees with the Panel that the federal government provide only aggregated data to requesting officials.[22] If the Commission adopts the Panel's recommendation that it be the point of contact for communications outage information in the wake of an emergency,[23] AT&T recommends that the Commission promulgate rules similar or identical to DHS's protected CII rules.

After a disaster has been declared, the importance of streamlining a communications provider's reporting obligations among various jurisdictions, while protecting carrier-specific data, cannot be overstated. To that end, AT&T recommends that the Commission work with state and local government associations to encourage their members to agree on the following approach upon the President declaring a major disaster or emergency: States in the affected areas would agree to suspend their *routine* outage reporting obligations in exchange for carrier-specific outage and infrastructure information that communications providers would voluntarily provide to the Commission, which would be subsequently shared with them. To expedite their access to this confidential information, the Commission, DHS, and industry should work with

[20] 6 U.S.C. § 133(a)(1)(A); *see also* section 214 of the Critical Infrastructure Information Act of 2002. Pub.L. 107-296, 116 Stat. 2150 (2002).
[21] 6 C.F.R. § 29.8(b). DHS defines "protected CII" as "CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in § 29.5." 6 C.F.R. § 29.2. It is our understanding that these interim rules will be made final by the end of the year.
[22] Panel Report and Recommendations at 34.
[23] *Id.* at 33.

these associations to establish a process to secure these written authorizations or non-disclosure agreements in advance of a disaster.

IV. A NATIONAL CREDENTIALING PROGRAM IS ESSENTIAL AND TELECOMMUNICATIONS INFRASTRUCTURE PROVIDERS SHOULD BE DESIGNATED EMERGENCY RESPONDERS.

Credentialing. The absence of a nationally recognized credential was a significant impediment to the communications industry's ability to quickly restore facilities damaged by Hurricanes Katrina and Rita. As the Panel recognized in its report, credentials recognized by one jurisdiction or one law enforcement agency were not consistently recognized by other jurisdictions or other law enforcement agencies.[24] The Panel notes that, not only were providers' employees and contractors not able to consistently access their company's facilities inside the affected areas, but equipment that was functioning after the hurricanes made landfall in some cases stopped functioning because the fuel and water truck drivers that the carriers retained to provide these necessities were unable to gain access to the area.[25]

To remedy this problem, AT&T proposes both a short-term and a long-term solution. The short-term solution to the credentialing problem is for the Commission to encourage states and private industry to follow the lead of Louisiana's and Georgia's Critical Infrastructure Owners/Operators Pilot Access Program.[26] Both the Georgia Office of Homeland Security and the Louisiana Office of Homeland Security and Emergency developed with DHS a pilot program to be tested in both states during the 2006 hurricane season. As a part of this program, the states identified essential elements for access into a restricted area for both critical infrastructure owners and operators ("CI/OO") and their contractors, subcontractors, and assigns. The following will be recognized by law enforcement and other state and local government officials

[24] *See id.* at 15-17.
[25] *Id.* at 17.
[26] *See* Appendix.

in Louisiana and Georgia and will ensure CI/OO access to restricted areas during a disaster: company issued photo ID; marked company vehicles; and letter of access issued by the company stating that the bearer is an authorized responder to the event. For contractors, subcontractors, and assigns of the CI/OO, the following documents will permit access to the restricted area: state-issued vehicle "hang tags" or placards, which the state will issue to any requesting CI/OO; employer-issued photo ID; letter of access from the CI/OO stating that the bearer is an authorized responder to the event, and providing a contact name and phone number for validation purposes.[27] Because dissemination of this SOP to state and local responders is essential, the state, CI/OO in the state, and DHS have each been tasked with important outreach activities. AT&T recommends that the Commission and DHS encourage other states to implement similar programs.

The long-term solution to the credentialing problem is adoption of a national credentialing standard. AT&T supports the findings of the National Security Telecommunications Advisory Committee ("NSTAC") in this regard and agrees with the Panel that these credentials should be made available to all communications infrastructure providers.[28] Among other things, NSTAC found that a standard credential must: employ tamper-proof, certificate-based picture identification technology to permit positive identification; support both physical and logical access of these screened individuals to critical telecommunications facilities; and be accepted throughout the government.[29] AT&T recommends that the Commission work with both DHS and other federal agencies to speed deployment of the National Institute of

[27] *See* Georgia Standard Operating Procedure ("SOP") at 1.
[28] *Id.* at 34.
[29] *See* National Security Telecommunications Advisory Committee, Trusted Access Task Force, *Screening, Credentialing, and Perimeter Access Controls Report*, at 4-6 (rel. Jan. 19, 2005).

Standards and Technology's Federal Information Processing Standard 201 ("FIPS 201") and with states to encourage them to recognize and accept this standard.[30]

Emergency Responder Designation. As recognized by the Panel, compounding the lack of a consistently recognized credential was the inability of telecommunications infrastructure providers to secure non-monetary federal assistance, such as security protection and priority access to restricted disaster sites.[31] AT&T supports the Panel's recommendation that telecommunications infrastructure providers be designated "Emergency Responders (Private Sector)" pursuant to the Stafford Act and DHS's National Response Plan, and AT&T encourages the Commission to work with the White House, DHS and Congress to implement this recommendation as quickly as possible.[32] If telecommunications infrastructure providers had been designated emergency responders prior to Hurricane Katrina, there would have been no question about their ability to receive security assistance from the National Guard and priority access to essential resources (*e.g.*, fuel, water, power, shelter) and restricted areas.[33] The adoption of this recommendation will enable communications providers to expedite their restoration efforts during future emergencies.

---

[30] Panel Report and Recommendations at 34; http://fips201ep.cio.gov/; http://csrc.nist.gov/piv-program/; State of Louisiana Standard Operating Procedure, Statewide Credentialing/Access Program at 2-3 (describing FIPS 201 and its usage by state and local governments).

[31] Panel Report and Recommendations at 18.

[32] *Id.* at 35.

[33] *See* National Security Telecommunications Advisory Committee, Legislative and Regulatory Task Force, *Federal Support to Telecommunications Infrastructure Providers in National Emergencies, Designation as "Emergency Responders (Private Sector),"* at 5-8 (rel. Jan. 31, 2006). It is also important that, once given access to restricted areas, employees of the telecommunications infrastructure providers be permitted to continue their restoration efforts after any curfew.

V. FIRST RESPONDER COMMUNICATIONS.

In its report, the Panel identified several areas affecting first responder communications that are in need of improvement.[34] AT&T will focus the majority of its comments on ways to enhance the resiliency of E-911 infrastructure and Public Safety Answering Points ("PSAPs"). AT&T generally supports the Panel's recommendations on these issues,[35] most of which are based on NRIC's best practices. As discussed below, however, in several instances, implementation of the Panel's recommendations may raise significant technical and operational challenges. Moreover, AT&T believes that in order to achieve the goals identified by the Panel, public safety agencies must move to IP-based, Next Generation 911 ("NG911") technology. Such a transformation will likely require a cooperative effort on the part of local, state and federal stakeholders. It will also require funding. While the Commission cannot provide the needed funding, it can and should be ready to lend its expertise to those states and localities committed to deployment of NG911 infrastructure. AT&T hopes that the momentum generated by the Panel's recommendations provides the opportunity to build reliability into the nation's 911 infrastructure while at the same time upgrading and enhancing it as described below. Only a funding plan at the federal level together with improved coordination within the states can make this possible.

Diverse Transport Facilities. AT&T's normal operating practice is to route 911 traffic between its 911 selective routers ("911 SR") and AT&T's local end office serving the PSAP over diverse interoffice transport facilities, when those facilities are available. In most cases, self-healing ring technology is deployed between AT&T's central offices, which greatly reduces the probability that an end office will be isolated from the 911 SR. When the 911 SR is provided

[34] *See* Panel Report and Recommendations at 22-27.
[35] *Id.* at 39-40.

by AT&T, AT&T recommends to interconnecting carriers that they route their 911 trunks over diverse facilities, if available. Not all local exchange carriers ("LECs"), however, are willing and able to bear the additional cost of diverse interoffice transport facilities for their 911 service.

From the local serving end office, PSAPs are generally served by copper cables, which means that there is less of a chance for facility diversity. Very few PSAPs have diverse entrance facilities; thus, even when the LEC provides diversity leaving the serving end office, there remains a single point of possible facility failure at the PSAP. AT&T recommends that PSAPs routinely review their 911 networks with their service providers and identify any points where facilities are not diverse. PSAPs should determine the best way to cost effectively mitigate this risk. Mitigation could include purchasing diverse facilities (which could be costly and may involve additional construction charges) or establishing a contingency plan, such as a back-up PSAP, for handling 911 calls if the PSAP were to be isolated due to a network outage.

Back-up Power. It is considered a best practice for LECs to have back-up batteries and/or diesel generators in every central office. During most emergencies, therefore, central offices are able to maintain constant telecommunications services within the community for a limited period of time after the loss of commercial power. All of AT&T's central offices are equipped with back-up batteries and/or diesel generators. AT&T recommends that PSAPs maintain their own back-up power just as AT&T does in its central offices. When AT&T provides the PSAP Customer Premise Equipment AT&T strongly encourages the 911 Authority to supply adequate back-up power systems at the PSAP.

Dual Active 911 SR Architecture. While it is possible to implement an architecture that is more robust and reliable using dual active 911 SR, creating a duplicative network is a very costly undertaking. Indeed, AT&T has deployed only two such networks, both done at the request and

expense of the governing 911 Authority. Other 911 Authorities have considered dual active 911 SRs, but ultimately determined that a complete duplication of their existing 911 network infrastructure was cost prohibitive. An alternative approach that may be more cost effective would be to implement a 911 network utilizing an IP next generation network (*i.e.*, NG911). Since IP technology is a distributed architecture, there are many more possibilities to provide redundancy and diversity than in the legacy TDM network. The NG911 architecture eliminates switched-based SRs and integrates routing functions that are distributed across the network. For this reason, AT&T suggests that a next generation solution would better serve the public interest than dual active 911 SRs. AT&T's recommendation that 911 Authorities implement NG911 is consistent with the National Emergency Number Association's proposed i3 architecture and its NG911 Plan.[36]

Secondary Back-up PSAP. AT&T supports the concept of establishing back-up PSAPs.[37] AT&T works with each PSAP that uses our 911 SR services to establish contingency routing procedures. In order to utilize a secondary back-up PSAP, there must be working transport facilities between the disaster area and the secondary back-up PSAP. Also, to be fully effective, the back-up location must be able to accommodate the call volume from the affected PSAP and must be able to respond appropriately to the calls received. In other words, the back-up PSAP must have the network, equipment, personnel, and training necessary to receive 911 calls with Automatic Location Information, determine the appropriate emergency response, communicate

[36] Initial Findings and Recommendations of NENA's NG E9-1-1 Program at 4 ("NENA's 9-1-1 Future Path Plan also proposed a hierarchy of interconnected local, regional and national IP networks that would enable NG 9-1-1 and many other emergency communications applications. The resulting model is a set of coordinated applications on an IP internetwork that serves multiple governmental functions and seamlessly interfaces voice and electronic data. In addition to improving response for daily emergencies, such a model would also improve homeland security by providing a nationally coordinated emergency response system."), *at* http://www.nena.org/media/files/ng_final_copy_lo-rez.pdf.

[37] Panel Report and Recommendations at 39.

with the first responders from and dispatch personnel to the disaster area served by the affected PSAP. Based on AT&T's experience, back-up PSAPs are generally located in close proximity to the PSAP that they are supporting. This model is ideal for most incidents such as PSAP-specific outages and localized disasters. The close proximity of the back-up PSAP allows full network connectivity, facilitates emergency staffing, and lessens the possibility of interoperability issues with dispatching and communications systems. This has proven to be operationally efficient and cost effective.

For large scale, catastrophic disasters such as Hurricane Katrina, the localized back-up PSAP approach will not suffice. A secondary back-up PSAP plan is an excellent idea that, if properly implemented, could be extremely effective in the event of a disaster even as large as Hurricane Katrina. Due to the large number of PSAPs in the United States, deploying geographically isolated, fully functional secondary back-up PSAPs on a one-to-one basis would strain the limits of both today's 911 architecture and the finances of the 911 Authorities. Therefore, AT&T recommends that secondary back-up PSAP plans be regional in scope and include contingency plans that will support all PSAPs in the region using one or more designated secondary back-up PSAP locations depending on the location and magnitude of the disaster. The identification of this secondary back-up PSAP should be based on capability, functionality and interoperability and not simply the Panel's proposed 200-mile threshold.[38] The development and implementation of a regional secondary back-up PSAP plan will facilitate coordinated, prioritized emergency response and will ensure that no PSAP is overlooked or omitted.

It is important to note that the network infrastructure required to support a fully featured, secondary back-up PSAP that is approximately 200 miles or more away generally does not exist today and may not be technically or operationally feasible in many cases. In implementing the

[38] *Id*

Panel's secondary back-up PSAP recommendation, one should consider not only the distance from the disaster, but the size of the distant PSAP and its ability to handle additional traffic loads. This latter point will almost always mean routing traffic to larger, metropolitan area PSAPs that can more easily accommodate additional loads. The larger metropolitan areas also have the benefit of easier access to communications and transportation systems, as well as additional labor forces. Dividing the country into regions and pre-determining back-up assignments is a major first step that must be initiated at the federal level and detailed at the state/jurisdictional level. Finally, AT&T recommends that the Commission evaluate alternatives that include next generation IP-based emergency services networks in order to provide fully featured, secondary back-up PSAP services in remote locations.

VI. CONCLUSION

For the foregoing reasons, AT&T urges the Commission to consider its proposals as outlined above.

Respectfully Submitted,

/s/ Cathy Carpino
Cathy Carpino
Gary Phillips
Paul K. Mancini

AT&T Inc.
1120 20th Street, NW
Suite 1000
Washington, D.C. 20036
(202) 457-3046 – phone
(202) 457-3073 – facsimile

Its Attorneys

August 07, 2006

APPENDIX

Standard Operating Procedure

Critical Infrastructure Owners/Operators
Pilot Access Program

2006 Hurricane Season

DRAFT v3.1

The CI/OO Pilot Access SOP is based solely on the authority of the state government.

Summary

This document outlines a model Standard Operating Procedure (SOP) for emergency response and management personnel at the State and local level in conjunction with critical infrastructure owners and operators (CI/OO) and their contractors, subcontractors, and assigns. This SOP seeks to clarify the roles, responsibilities and processes that will be followed to ensure that critical infrastructure providers are given timely and efficient access to hurricane or other disaster-affected areas for the purpose of repairing the infrastructure. This document is a product of a joint Federal, State, County, local and private sector efforts to ensure the timely functionality of critical infrastructure for citizens. This SOP was developed in partnership with the State of Georgia Office of Homeland Security-Georgia Emergency Management Agency (OHS-GEMA) and will be pilot tested in Georgia during the 2006 hurricane season.

Process Overview

All participants agree that the following criteria are essential elements for access into a restricted area during a hurricane or other natural disaster.

For Critical Infrastructure Owners and Operators

- Company-issued photo ID
- Marked Company vehicles
- Letter of Access issued by the Company stating that the Bearer is an authorized responder to the event

For Contractors, Subcontractors, and Assigns of the CI/OO

- State-issued vehicle “hang tags” or placards
- Employer-issued photo ID
- Letter of Access from the CI/OO stating that Bearer is an authorized responder to the event, and providing a contact name and phone number for validation purposes

Prior to the beginning of Hurricane Season, the State of Georgia will issue motor vehicle hang tags to any requesting CI/OO entity. The CI/OO will be responsible for the dissemination of these identifiers for its contractors, subcontractors, and assigns.

SECTION I — INTRODUCTION

A. PURPOSE

The purpose of this CI/OO Access Standard Operating Procedure [SOP] document is to describe in concept the joint Federal, State, County and local Infrastructure strategy to permit access into restricted areas during the 2006 Hurricane season. This SOP is intended for Federal, state, local representatives and private sector companies (critical infrastructure owners/operators) in Georgia and to serve as an operational model for other states and municipalities.

SECTION 2 – CONCEPT OF OPERATIONS

A. IDENTIFICATION PROCEDURES

Federal, state and local government agencies and law enforcement officials agree to recognize specific identification from critical infrastructure owners and operators, and their contractors, subcontractors, and assigns as they seek access into a restricted disaster area.

In furtherance of the CIP Access Program, Federal, state and private sector partners all agree to take action in support of this SOP. The following actions are required:

Critical Infrastructure Owner/Operators (for own employee base):

- Ensure Company-issued photo ID for each employee
- Ensure Company vehicles are marked
- Issue Letter of Access issued by the Company stating that the Bearer is an authorized responder to the event
- Promote the use of this SOP at the State and local level

Critical Infrastructure Owner Operator (for Contractors, Subcontractors, and Assigns):

- Obtain State-issued vehicle “hang tags” or placards
- Ensure Employer-issued photo ID for each employee
- Provide Letter of Access from the CI/OO stating that Bearer is an authorized responder to the event, and providing a contact name and phone number for validation purposes

State:

- Identify location and point of contact to obtain hang tags or placards
- Disseminate “hang tags” or State placards available prior to Hurricane season
- Provide this SOP to State response personnel, and where appropriate, local response personnel

Local:

- Educate personnel on the existence of the SOP
- Coordinate with CI/OO in the jurisdiction on the SOP

Federal:

- Educate Federal response personnel on the existence of the SOP

B. LETTER OF ACCESS AUTHORIZATION PROCESS

There one type of access letter that can be issued to facilitate entry into a restricted area:

Critical Infrastructure Owner Operator Letters:
The CI/OO will create and distribute Letters of Access (LOA) on company letterhead to all employees seeking access to areas where routes have been deemed passable but not open to the general public. Similarly, companies will prepare letters for contractors, subcontractors, and assigns, which similarly authorize access on behalf of the CI/OO into an open but restricted area. These letters authorize the bearer of the LOA to enter the restricted area for the purpose of assessing damage to and restoring the infrastructure, and will include a CIP point of contact (name/telephone number) for validation purposes.

C. GEORGIA VEHICLE IDENTIFICATION TAGS

Prior to the start of the 2006 Hurricane Season, GA OHS/GEMA will issue vehicle identification tags or placards to primary critical infrastructure providers and Georgia counties (for local distribution). These hang tags or placards will be made available for companies to disseminate. Companies can use these hang tags for unmarked vehicles, or to support contractors, subcontractors, and assigns acting on behalf of the CI/OO responding to the crisis.

The State of Georgia will issue tags with serial numbers. The State will record the serial numbers issued to each CI/OO, and CI/OO entities are required to do the same. Hang tags are available from the GEMA Operations Division (404) 635-7000. Hang tags are available after May 15, 2006, and are valid for the entire Hurricane Season.

D. OUTREACH

This program is a part of the public-private partnership. As such, outreach obligations exist for all parties involved. Critical Infrastructure owners and operators are responsible for training their employees, contractors, sub-contractors, and assigns. As disasters are local in nature, CI/OO entities are also responsible for outreach to local responders, to make them aware of this process. At the state level, Georgia

OHS/GEMA will ensure that required State officials and responders are made aware of this SOP, and will disseminate this information to the local level. County, local and municipal persons are responsible for partnering with CI/OO and State representatives in support of this initiative. At the Federal level, DHS will work to ensure that all Federal protection representatives are aware of this SOP and will support dissemination of this SOP throughout the United States.

State of Georgia

Critical Workforce Disaster Re-Entry Permit

06

Expires 12/06

Issued by the
Georgia Office of Homeland Security-
Georgia Emergency Management Agency

Misuse of this Permit Constitutes Fraud

STATE OF LOUISIANA

STANDARD OPERATING PROCEDURE

Statewide
Credentialing/Access Program

2006 All Hazards Access

June, 2006

STATE OF LOUISIANA

STANDARD OPERATING PROCEDURE

Critical Infrastructure Owners/Operators
Pilot Access Program

2006 All Hazards Access

SUMMARY

Hurricane Katrina revealed a need for uniform reentry criteria for essential personnel entering a closed emergency area post disaster event. Lack of uniform access guidelines resulted in delays and loss of critical utilities and services, as well as delays in reestablishing security and communications systems following Katrina.

This document outlines a model Standard Operating Procedure (SOP) for emergency response and management personnel at the State and local level in conjunction with critical infrastructure owners and operators (CI/OO) and their contractors, and other personnel. This SOP seeks to clarify the roles, responsibilities, and processes that will be followed to ensure that critical infrastructure providers are given timely and efficient access to hurricane or other disaster-affected areas for the purpose of repairing the infrastructure. This document is a product of a joint Federal, State, Parish, local and private sector effort to ensure the timely functionality of critical infrastructure for citizens. This SOP was developed by the Louisiana State Police in partnership with the State of Louisiana Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP), the National Department of Homeland Security, and the Louisiana Sheriffs and Chiefs of Police Associations.

Homeland Security Presidential Directive 12 (HSPD 12), dated August 27, 2004, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors," directed the promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. It further specified secure and reliable identification that, among other things:

1. Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
2. Can be rapidly authenticated electronically
3. Is issued only by providers whose reliability has been established by an official accreditation process.

The "Federal standard" referenced above is the Federal Information Processing Standard 201(FIPS 201). FIPS 201 technology uses a card with an Integrated Circuit Chip (ICC) (commonly called a smart card) which uses Public Key Infrastructure (PKI) for identity and attribute (qualification, certification, authorization, and/or privilege) authentication ensuring that the responder is who s/he says s/he is and that they truly possess the attribute(s) they say they do. Although this is a Federal standard, many State and local governments in the National Capital

Region (NCR) and throughout the country are adopting this standard to enable nation-wide interoperability. FIPS 201 standard compliance will be an ongoing project with full implementation of standardized credentials by 2008 and will be incorporated in the next version of this SOP.

It is anticipated that reentry will occur in a tiered approach, based on key roles, in restoring normal operations after a disaster. Admittance will be granted based on the immediate needs and requirements of the locally affected area through the local EOC and Parish and State Governments. Tier 1 will include Search and Rescue Personnel, Infrastructure and Utilities Repair Personnel, Official Damage Assessment Teams, and other personnel at the discretion of the State, Parish, and local jurisdictions; Tier 2 will include Relief Workers (e.g. Red Cross Volunteers), Healthcare Agencies (to include Volunteer Health Professionals (VHPs), Banking Organizations, Insurance Agencies, and Businesses deemed to be essential to the recovery effort; and Tier 3 will include Businesses not included in Tier 2 and residents.

PROCESS OVERVIEW

All participants agree that the following criteria are essential elements for access into a restricted area during a hurricane or other natural disaster and will be administered ONLY in the event of a Declaration/State of Emergency from the Governor or affected Parish President/Mayor when a mandatory evacuation order has been issued. It is imperative that local governments are familiar with utility and critical infrastructure needs and are aware of, based on the disaster, which critical infrastructure agencies (to include the Louisiana National Guard and the United States Coast Guard) will need immediate access to the affected area.

The following is a listing of identification that will be required to gain access at checkpoints:

Critical Infrastructure Owners and Operators, to include Contractors, Subcontractors, and Personnel of the CI/OO, must have the following identification:

1. A valid State Drivers License and company-issued photo ID
2. Marked Company vehicles (companies should have standardized markings)
3. Letter of Access (LOA) issued by the company (with verified phone number) stating that the bearer and vehicle is an authorized responder to the event.

Federal Bureau of Investigation (FBI)-issued INFRAGARD credentials, the Department of Defense (DOD) Common Access Cards (CACs), and FIPS 201 compliant identification credentials issued by Federal government agencies will be acceptable forms of identification.

SECTION I—INTRODUCTION

PURPOSE

The purpose of this CI/OO Access SOP document is to describe in concept the joint Federal, State, Parish and local infrastructure strategy to permit access into restricted areas during the 2006 Hurricane Season. This SOP is intended for Federal, State, local representatives and private sector companies (critical infrastructure owners/operators) in Louisiana and to serve as an operational model for other States and municipalities.

SECTION II—CONCEPT OF OPERATIONS

A. REENTRY PROTOCOL

It is anticipated that reentry will occur in a tiered approach based on key roles in restoring normal operations after a disaster. It is understood that events that may occur within specific jurisdictions will dictate, based on local needs and factors, what personnel will need access into the affected area. Safety, with regard to public health, travel accessibility and rescue operations will be paramount and of crucial importance in determining any access.

- **(Immediate and unrestricted access) will be granted to Search and Rescue Agents, including agents from Parish and Municipal Fire-Rescue Departments, State, Local and Federal Law Enforcement, Fire/EMS, National Guard (Military), and Emergency Response Agencies in support of efforts in the affected area.**

Tier I

- Infrastructure and Utilities Repair Personnel: These agencies must be permitted immediate access to ensure that essential services such as water, lighting, and communications are restored and infrastructure is intact. Municipal utilities and public works personnel also are included.

- Official Damage Assessment Teams: These may include FEMA, State, and local officials.

- Other personnel at the discretion of the Parish Department of Homeland Security or applicable municipal Emergency Operations Center (EOC).

Tier 2

- Relief Workers: These groups will be needed to provide food and other supplies for people in impacted areas who did not evacuate.

- Healthcare Agencies: These include hospitals, nursing homes, assisted living facilities, and dialysis centers. Additionally, includes Volunteer Health Professionals (VHPs) with valid, approved identification documentation.

- Insurance Agents.

- Banking Organizations.

- Business operators considered critical to the recovery effort. Parish and municipal officials will make the decision to permit key business operators to return to impacted areas based on an overall evaluation of the situation. Key business operators will be allowed to reenter their communities when the governing jurisdictions, in consultation with the Parish Department of Emergency Management, agree that the following factors are resolved:

  a. Access: Major routes are intact and passable.

  b. Public Health: There is no threat to public safety.

  c. Rescue: All search and rescue operations have been completed.

- Other personnel at the discretion of the Parish Department of Homeland Security or applicable municipal Emergency Operations Center (EOC).

Tier 3

Business operators now allowed in under Tier 2, and residents will be allowed to return as areas are deemed safe.

B. IDENTIFICATION PROCEDURES

Federal, State, and local government agencies and law enforcement officials agree to recognize specific identification from critical infrastructure owners and operators, and their contractors, subcontractors and assigns as they seek access into a restricted disaster area. Relying parties (e.g. law enforcement, National Guard) will require constant communications with local and State EOCs so that proper admittance is granted. Once identity and attributes are authenticated, access is granted at the discretion of the relying parties. In furtherance of this access program, Federal, State, and private sector partners all agree to take action in support of this SOP. The following actions are required:

Critical Infrastructure Owner/Operators (for Employees and Contractors, Subcontractors, and affected Personnel):

- Ensure possession of valid identification card to include attributes
- Ensure Company vehicles utilize standard markings and LOA
- Promote the use of this SOP at the State and local level

Emergency Response/Emergency Medical/Law Enforcement/Fire/Military Personnel:

- A uniformed Law Enforcement/EMS/Emergency Response/Fire/Military personnel with valid identification card to include attributes

- A properly marked or identified Law Enforcement/EMS/Emergency Response/Fire/Military vehicle with commissioned or credentialed occupant
- Unmarked Agency vehicle with proper identification as stated above

State:

- Provide this SOP to State response personnel, and where appropriate, local response personnel
- Ensure that local EOCs are aware of and maintain an updated, current list of critical infrastructure personnel, to include attribute(s), within their Parish
- Make every effort to expedite the movement of critical infrastructure personnel into an affected area

Local:

- Educate local response personnel on the existence and requirements of the SOP
- Maintain an updated, current list of critical infrastructure personnel, to include attribute(s), and contact person within the Parish
- Communicate with State on non-acceptance or special requirements for access by critical infrastructure within the local Parishes
- Facilitate adjoining Parishes, absent an emergency, with the movement of critical infrastructure personnel into an affected area

Federal:

- Educate Federal response personnel on the existence of the SOP
- FBI will administer INFRAGARD program

C. OUTREACH

This program is part of the public-private partnership. As such, outreach obligations exist for all parties involved. Critical infrastructure owners and operators are responsible for training their employees, contractors, subcontractors and assigns. Contractors, as well as owner operators, should take measures to ease entrance into affected area by prior coordination with Emergency Officials from the affected area and the Louisiana State Police. As disasters are local in nature, CI/OO entities are also responsible for outreach to local responders, to make them aware of this process. At the State level, Louisiana OHS/GOHSEP and the Louisiana State Police will ensure that required State officials and responders are made aware of this SOP and will disseminate this information to the local level. Parish, local and municipal persons are responsible for partnering with CI/OO and State representatives in support of this initiative.

D. FBI INFRAGARD

The FBI INFRAGARD program qualifies membership through a State and Federal criminal record check and most importantly, an FBI record check for associations with threat organizations. Once vetted, INFRAGARD members are granted a membership identification card. The State and regional critical industry representatives have asked for this identification to facilitate a private credentialing plan for non-EMS and non-utility vehicle access.

The Louisiana INFRAGARD credentials are to be honored and utilized only after disasters where local and/or State authorities have declared a State of Emergency thereby restricting access into an affected area. These credentials are carried by State and Federal verified non-law enforcement personnel who are essential to maintaining operations of critical infrastructure such as medical, power, gas, chemical, communication (wireless and landline), transportation and financial facilities.

Each INFRAGARD member requesting entry into an affected area must present an INFRAGARD membership identification card along with a verbal explanation of the reason for reentry.